



Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO				Complete if Known	
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  (use as many sheets as necessary)				Application Number	09/966,224
				Filing Date	2
				First Named Inventor	Michael D. Ruehle
				Art Unit	2134 2-136
				Examiner Name	Not yet assigned COLIN
				Attorney Docket Number	42390.P11974
Sheet	1	of	2		

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. 1	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number - Kind Code <sup>2</sup> (if known)			
ce		us- 4,218,582		Hellman et al.	
ce		us- 4,707,800		Montrone et al.	
ce		us- 4,737,926		Vo et al.	
ce		us- 4,914,617		Putrino et al.	
ce		us- 5,047,975		Patti et al.	
ce		us- 5,189,636		Patti et al.	
ce		us- 5,289,397		Clark et al.	
ce		us- 5,327,369		Ashkenazi, Yaron	
ce		us- 5,623,683		Pandya, Ashish	
ce		us- 5,870,478		Kawamura, Shinichi	
ce		us- 6,035,317		Guy, Monier	
ce		us- 6,061,706		Gai et al.	
ce		us- 6,151,393		Jeong, Yong-Jin	
ce		us- 6,209,016 B1		Hobson et al.	
ce		us- 6,240,436 B1		McGregor, Matthew Scott	
		us-			
		us-			
		us-			
		us-			
		us-			

[illegible]

Examiner Signature	<i>Paul Lohr</i>	Date Considered	9/16/05
-----------------------	------------------	--------------------	---------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 18 if possible. <sup>6</sup> Applicant is to place a check mark here if English language Translation is attached.

**Burden Hour Statement:** This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.**



PTO/SB/08B (10-01)

Approved for use through 10/31/2002. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no person is required to respond to a collection of information unless it contains a valid OMB control number.

+

Substitute for form 1449B/PTO		<b>Complete if Known</b>	
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  (use as many sheets as necessary)		Application Number	09/966,224
		Filing Date	September 28, 2001
		First Named Inventor	Michael D. Ruehle
		Group Art Unit	2131 2136
		Examiner Name	Not yet assigned CALIN
Sheet	2	of	2
		Attorney Docket Number	42390.P11974

OTHER PRIOR ART - NON PATENT LITERATURE DOCUMENTS			
Examiner Initials <sup>1</sup>	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T <sup>2</sup>
ec		Bajard, Jean-Claude et al., "An RNS Montgomery Modular Multiplication Algorithm", Abstract, November 1996, pages 1-10	
ec		Blum, Thomas, "Modular Exponentiation on Reconfigurable Hardware", Thesis submitted to the Faculty of the Worcester Polytechnic Institute, April 8, 1999	
ec		Koc, Cetin Kaya, "RSA Hardware Implementation", Version 1.0, August 1995, pages 1-28	
ec		Rivest, R.L. et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Abstract, pages 1-15	

Examiner Signature	<i>David H. Hines</i>	Date Considered	9/16/01
--------------------	-----------------------	-----------------	---------

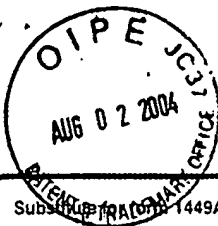
\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

+





Substantive Patent 1449A/PTO		Complete If Known	
		Application Number	09/966,224
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date	September 28, 2001
		First Named Inventor	Michael D. Ruehle
		Art Unit	<del>2131</del> 2136
		Examiner Name	<del>Not Yet Assigned</del> COLIN
		Attorney Docket Number	42390P11974
Sheet	2	of	2

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.†	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T*
cc	3	KATO T ET AL: "A Design for Modular Exponentiation Coprocessor in Mobile elecommunication Terminals", Cryptographic Hardware and Embedded Systems. 2nd International Workshop, CHES 2000, Worchester, MA, Aug. 17-18, 2000, pages 516-228, XP001049135.	
cc	4	BLUM ET AL: "High-Radix Montgomery Modular Exponentiation on Reconfigurable Hardware, IEEE Trans. Comput. (USA), IEEE Transaction on Computers, July 2001, IEE, USW, vol 50, no. 7, July 2001, pages 759-765, XP002283657.	
cc	5	IWAMURA K ET AL: "Montgomery Modular-Multiplication Method and Systolic Arrays Suitable for Modular Exponentiation", Electronics & Communications in Japan, Part III - Fundamental Electronic Science Scripta Technica. New York, US, vol 77, no 3, March 1, 1994, pages 40-50, XP000468346.	

RECEIVED

AUG 06 2004

Technology Center 2100

Examiner Signature	<i>Carol [Signature]</i>	Date Considered	9/16/05
--------------------	--------------------------	-----------------	---------

\*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication.

†Applicant's unique citation designation number. \*Applicant is to place a check mark here if English language Translation is attached.

Based on PTO/SB/08B (08-03) as modified by Blakely, Solokoff, Taylor & Zalman (w/r) 08/11/2003.  
Send To: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450